REMARKS

Claims 17-66 and 92-112 are pending in the present application. Claim 93-112 have bean added as a result of this response. Claims 17, 22, 27, 32, 37, 42, 47, 52, 57, and 62 are independent claims.

OBJECTION TO THE TITLE

In accordance with the Examiner's suggestion, Applicants have amended the title to recite "A MULTIPRIME RSA PUBLIC KEY CRYPTOSYSTEM". Reconsideration and withdrawal of this objection is respectfully requested.

INFORMAL DRAWINGS

Applicants acknowledge the Examiner's indication that the present application has been filed with informal drawings and that formal drawings will be required when the application is allowed.

35 U.S.C. § 103(A) LIDL/QUISQUATER/RIVEST ET AL. REJECTION

Claim 17 has been rejected under 35 U.S.C. § 103(a) as being unpatentable over Lidl and Pilz (Applied Abstract Algebra, 1984), and further in view of Quisquater and Couvreur, Fast Dicpherment Algorithm for RSA Public-Key Cryptosystem, 1982); and Rivest et al., A Method for Obtaining Digital Signatures and Public-key Cryptosystem, Communications of the ACM, 21(2) February 1978, henceforth Rivest. This rejection, insofar as it pertains, to the presently pending claims, is respectfully traversed for the following reasons.

In formulating the rejection of claim 17 in view of Lidl, Quisquater, and Rivest, the Examiner picks and chooses various portions of three publications to piece together the subject matter of the present claims. Applicants assert that it is impermissible to use the claimed invention as an instruction manual or template to piece together the teaching of the prior art so that the claimed invention is rendered obvious. It is established U.S. Patent Law that one cannot use hindsight reconstruction to pick and choose among isolated disclosures in the prior art to deprecate the claimed invention. Obviousness cannot be established by combining the teachings of the prior art to produce the claimed invention, absent a teaching or suggestion supporting the combination. Under § 103, the teachings of references can be combined only if there is some suggestion or incentive to do so. Applicants respectfully submit that the Examiner has not set forth any reasons why one of ordinary skill in the art would pick and choose various teachings of Lidl, Quisquater, and Rivest, in order to piece together the invention recited in the presently pending claim. Accordingly, Applicants respectfully submit that claim 17 is allowable for at least this reason.

35 U.S.C. § 103(A) LIDL/QUISQUATER/RIVEST ET AL./DING ET AL. REJECTION

Claims 18-66 and 73-92 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over Lidl and Pilz (Applied Abstract Algebra, 1984), and further in view of Quisquater and Couvreur, Fast Decipherment Algorithm for RSA Public -Key Cryptosystem, 1982); and Rivest et al., A Method for Obtaining Digital Signatures and Public-key Cryptosystem, Communications of the ACM, 21(2) February 1978, as applied to claim 17 above, and further in view of Ding et al. The Chinese Remainder Theorem, World Scientific. This

rejection, insofar as it pertains to the presently pending claims, is respectfully traversed for the following reasons.

In formulating this rejection in view of Lidl, Quisquater, Rivest, and Ding, the Examiner again picks and chooses various portions of four publications to piece together the subject matter of the present claims. Applicants assert that it is impermissible to use the claimed invention as an instruction manual or template to piece together the teaching of the prior art so that the claimed invention is rendered obvious. Applicants respectfully submit that the Examiner has not set forth any reasons why one of ordinary skill in the art would pick and choose various teachings of Lidl, Quisquater, Rivest, and Ding, in order to piece together the invention recited in the presently pending claim. Accordingly, Applicants respectfully submit that claims 18-66 and 73-93 are allowable for at least this reason.

35 U.S.C. § 103(A) RSA/RIVEST ET AL./QUISQUATER/KNUTH REJECTION

Claim 17 has been rejected under 35 U.S.C. § 103(a) as being unpatentable over Rivest et al. (US 4,405,829 A) henceforth RSA, and further in view of Rivest et al., A Method for Obtaining Digital Signatures and Public-key Cryptosystem, Communications of the ACM, 21(2) February 1978, henceforth Rivest; Quisquater, Fast Decipherment Algorithm for RSA Public-key Cryptosystem and further in view of Knuth, The Art of Computer Programming, Vol. 2, page 179. This rejection, insofar as it pertains to the presently pending claims, is respectfully traversed for the following reasons.

In formulating the rejection of claim 17 in view of RSA, Rivest, Quisquater, and Knuth, the Examiner picks and chooses various portions of four publications to piece together the subject matter of the present claims. Applicants assert that it is impermissible to use the claimed

invention as an instruction manual or template to piece together the teaching of the prior art so that the claimed invention is rendered obvious. Applicants respectfully submit that the Examiner has not set forth any reasons why one of ordinary skill in the art would pick and choose various teachings of RSA, Quisquater, Rivest, and Knuth in order to piece together the invention recited in the presently pending claim. Accordingly, Applicants respectfully submit that claim 17 is allowable for at least this reason.

35 U.S.C. § 103(A) RSA/QUISQUATER/RIVEST ET AL./DING ET AL. REJECTION

Claims 18-66 and 73-92 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over Rivest et al. (US 4,405,829 A) henceforth RSA, and further in view of Quisquater, Fast Decipherment Algorithm for RSA Public-Key Cryptosystem, 1982; and Rivest et al. A Method for Obtaining Digital Signatures and Public-key Cryptosystem, Communications of the ACM, 21(2) February 1978, as applied to claim 17 above, and further in view of Ding et al. The Chinese Remainder Theorem, World Scientific. This rejection, insofar as it pertains to the presently pending claims, is respectfully traversed.

In formulating the rejection of claim 18-66 and 73-92 in view of RSA, Quisquater, Rivest, and Ding, the Examiner picks and chooses various portions of four publications to piece together the subject matter of the present claims. Applicants assert that it is impermissible to use the claimed invention as an instruction manual or template to piece together the teaching of the prior art so that the claimed invention is rendered obvious. Applicants respectfully submit that the Examiner has not set forth any reasons why one of ordinary skill in the art would pick and choose various teachings of RSA, Quisquater, Rivest, and Ding, in order to piece together the

invention recited in the presently pending claim. Accordingly, Applicants respectfully submit that claims 18-66 and 73-92 is allowable for at least this reason.

35 U.S.C. § 1203(A) NEMO/RIVEST ET AL./QUISQUATER REJECTION

Claims 17 has been rejected under 35 U.S.C. § 103(a) as being unpatentable over Nemo, RSA Moduli Should Have 3 Primes Factors, August 1996; Rivest et al., A Method for Obtaining Digital Signatures and Public-key Cryptosystem, Communications of the ACM, 21(2) February 1978, henceforth Rivest; and Quisquater, Fast Decipherment Algorithm for RSA Public-key Cryptosystem, 1982. This rejection, insofar as it pertains to the presently pending claims, is respectfully traversed for the following reasons.

With respect to Nemo, Applicants respectfully assert that this publication was submitted by Applicants during prosecution of the original application with no date, since applicants were unable to ascertain the publication date of the Nemo paper. Nemo was printed on the front of U.S. Patent 5,848,159 with "No Date or Publication Given".

During the prosecution of the present application, the Examiner has adopted the publication date of Nemo as August 1996, relying on a footnote on page 1 which states "the original version of this article may be obtained from Scientific Bulgarian Magazine, August 1996". Applicants respectfully assert that the fact this paper was submitted by a pseudonym as "Captain Nemo" and alleges to have been published in a fictitious publication, namely "Scientific Bulgarian", casts sufficient doubt as the date of the publication to render it insufficient to be relied upon as prior art against the present application. As set forth in M.P.E.P. § 706.02(a), the Examiner must determine the issue or publication date of a reference of a proper comparison between the application and the reference dates can be made. Applicants respectfully assert that

the fictitious author in a fictitious journal, namely "Scientific Bulgarian", cast doubt on the accuracy of August 1996 as a publication date. Until the Examiner is able to verify the publication date of the Nemo publication as qualifying as prior art against the present application under 35 U.S.C. § 102(a) or (b) Applicants respectfully submit that Nemo cannot be applied against the present application. Accordingly, reconsideration and withdrawal of this rejection is respectfully requested.

Further, in formulating the rejection of claim 17 in view of Nemo, Quisquater, and Rivest, the Examiner picks and chooses various portions of three publications to piece together the subject matter of the present claims. Applicants assert that it is impermissible to use the claimed invention as an instruction manual or template to piece together the teaching of the prior art so that the claimed invention is rendered obvious. Applicants respectfully submit that the Examiner has not set forth any reasons why one of ordinary skill in the art would pick and choose various teachings of Nemo, Quisquater, and Rivest, in order to piece together the invention recited in the presently pending claim. Accordingly, Applicants respectfully submit that claim 17 is allowable for at least this reason.

35 U.S.C. § 1203(A) NEMO/QUISQUATER/RIVEST ET AL./ DING ET AL. REJECTION

Claims 18-66 and 73-92 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over Nemo, RSA Moduli Should Have 3 Primes Factors, August 1996, and further in view of Quisquater, Fast Decipherment Algorithm for RSA Public -Key Cryptosystem, 1982); Rivest et al., A Method for Obtaining Digital Signatures and Public-key Cryptosystem, Communications of the ACM, 21(2) February 1978, as applied to claim 17 above, and further in

view of Ding et al. The Chinese Remainder Theorem, World Scientific. This rejection, insofar as it pertains to the presently pending claims, is respectfully traversed for the following reasons.

With respect to Nemo, Applicants respectfully assert until the Examiner is able to verify the publication date of the Nemo publication as qualifying as prior art against the present application under 35 U.S.C. § 102(a) or (b), Applicants respectfully submit that Nemo cannot be applied against the present application. Accordingly, reconsideration and withdrawal of this rejection is respectfully requested.

In formulating the rejection of claim 18-66 and 73-92 in view of Nemo, Quisquater, Rivest, and Ding, the Examiner picks and chooses various portions of three publications to piece together the subject matter of the present claims. Applicants assert that it is impermissible to use the claimed invention as an instruction manual or template to piece together the teaching of the prior art so that the claimed invention is rendered obvious. Applicants respectfully submit that the Examiner has not set forth any reasons why one of ordinary skill in the art would pick and choose various teachings of Nemo, Quisquater, Rivest, and Ding, in order to piece together the invention recited in the presently pending claim. Accordingly, Applicants respectfully submit that claim 18-66 and 73-92 is allowable for at least this reason.

Applicants respectfully submit that the new claims 93-112 recite additional patentable features of the present invention. Allowance of claims 93-112 is respectfully requested.

CONCLUSION

Accordingly, in view of the above amendments and remarks, reconsideration of the objections and rejections and allowance of each of claims 17-66 and 73-112 in connection with the present application is earnestly solicited.

Pursuant to 37 C.F.R. §§ 1.17 and 1.136(a), Applicant(s) hereby petition(s) for a three (3) month extension of time for filing a reply to the outstanding Office Action and submit the required $950.00 extension fee herewith.

Should there be any outstanding matters that need to be resolved in the present application, the Examiner is respectfully requested to contact John A. Castellano at the telephone number of the undersigned below.

If necessary, the Commissioner is hereby authorized in this, concurrent, and future replies, to charge payment or credit any overpayment to Deposit Account No. 08-0750 for any additional fees required under 37 C.F.R. § 1.16 or under 37 C.F.R. § 1.17; particularly, extension of time fees.

Respectfully submitted,

HARNESS, DICKEY, & PIERCE, P.L.C.

By _____

John A. Castellano, Reg. No. 35,094
P.O. Box 8910
Reston, Virginia 20195
(703) 668-8000

JAC/cah